UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/922,209	08/03/2001	John David West Brothers	9339/34809	7950

24728 7590 02/09/2005

MORRIS MANNING & MARTIN LLP
1600 ATLANTA FINANCIAL CENTER
3343 PEACHTREE ROAD, NE
ATLANTA, GA 30326-1044

EXAMINER	
HOSSAIN, TANIM M	

ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/922,209	BROTHERS, JOHN DAVID WEST	
	Examiner	Art Unit	
	Tanim Hossain	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/13/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 4 and 14 are objected to because of the following informalities: "RDS" in claim 4, and "EAD" in claim 14 appear to be typographical errors. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 5, 6, 8-16, 21, 22, 39-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Skopp et al. (U.S. 6,256,739).

As per claim 1, Skopp teaches a method comprising the steps of: (a) generating hash data based on at least one of a universal resource locator of a resource, resource access rights data defining restrictions on a web access device, and/or user thereof to access the resource, and an internet protocol address of the WAD (column 6, lines 10-15; column 9, lines 29-43); and (b) combining hash data, URL, and resource access right data in a web page (column 9, lines 29-43).

As per claim 2, Skopp teaches a method as claimed in claim 1, further comprising the step of: transmitting the webpage document including the secure URL to the WAD in response to a request for the web page document from the WAD (column 9, lines 29-43).

As per claim 5, Skopp teaches a method as claimed in claim 1, wherein the resource access right data includes at least one of: 1) an authorized IP address of IP address range (column 9, lines 18-28); 2) lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid (column 10, lines 53-58); and/or 3) maximum reference data indicating a maximum number of times a web access device and/or user thereof can access a resource (column 10, lines 28-32).

As per claim 6, Skopp teaches a method comprising the steps of: at a resource provider subsystem, (a) receiving a request for a web page from a web access device via a network, the request including a network address of the web access device (column 9, lines 1-8); (b) determining resource access right data for the web access device and/or a user thereof, the resource access right data defining restriction(s) for the web access device and/or user thereof to access a resource (column 9, lines 9-17); (c) securing a URL for a resource by generating hash data based on at least one of the URL, a network address of the web access device, and/or resource access right data, and combining the URL, resource access right data, and hash data together in the webpage (column 9, lines 1-8, 29-43); and (d) transmitting the web page having the secure URL to the web access device via the network in response to the request received in step (a) from the web access device (column 9, lines 1-43).

As per claim 8, Skopp teaches a method as claimed in claim 6, wherein the network address of the web access device is an IP address (column 9, lines 26-29).

As per claim 9, Skopp teaches a method comprising the steps of: (a) receiving a signal requesting a web page document from a web access device, the signal including an IP address of the WAD (column 6, lines 4-14); (b) retrieving data for the web page document including a universal resource locator of a document referenced in the web page document (column 6, lines 4-14); (c) retrieving resource access right data for the URL using the IP address of the web access device and/or user name and password established through a log-in procedure (column 6, lines 35-38); (d) generating has and/or encrypted data to generate secure resource access right data (column 9, lines 29-43); combining the resource access right data with the respective URL to generate a secure URL (column 9, lines 1-43); (f) generating the web page document including the secure URL (column 9, lines 1-43); (g) transmitting the secure URL to the WAD (column 9, lines 1-43).

As per claim 10, Skopp teaches a method comprising the step of: at a web access device, (a) transmitting a signal requesting a web page document to a resource provider subsystem (column 6, lines 4-14); and (b) receiving the web page document having a secure universal resource locator with hash data, URL, and resource access right data, in response to the request (column 6, lines 4-14).

As per claim 11, Skopp teaches a method as claimed in claim 10 further comprising the step of: (c) activating the secure URL with the WAD to transmit a signal requesting access to a resource designated by the URL to a resource distribution subsystem (RDS) (column 9, lines 1-43); and (d) accessing the resource with the WAD if the RDS determines that access to the resource is authorized based on the hash data and resource access right data contained in the request signal (column 6; lines 4-14).

As per claim 12, Skopp teaches a method comprising the steps of: (a) at a web access device, generating and transmitting a request for a web page document to a resource provider subsystem (column 6, lines 4-14); (b) receiving the requested web page document having a secure universal resource locator with secured resource access right data from the resource provider subsystem (column 9, lines 1-43); (c) executing a browser application and web page document with the WAD to generate and transmit a signal to request a resource distribution subsystem to provide access to a resource identified by the secure URL, the request signal including the URL and secure resource access right data (column 9, lines 1-43); and (d) if access to the resource is permitted by the RDS, accessing the resource with the WAD (column 6, lines 4-14).

As per claim 13, Skopp teaches a method as claimed in claim 12, wherein the step (d) comprises the substeps of: (d1) receiving at the WAD resource data from the RDS (column 6, lines 4-14); (d2) storing the resource data in memory of the WAD (column 6, lines 4-14); (d3) executing an application with the WAD based on the resource data to generate a signal (column 6, lines 4-14); and (d4) generating a display with the WAD based on the signal generated in the substep (d3) (column 9, lines 1-8).

As per claim 14, Skopp teaches a method as claimed in claim 12, wherein the step (d) comprises the substeps of: (d1) receiving a program module resource from the RDS (6; 4-14); (d2) loading the program module resource into memory of the WAD (6; 4-14); (d3) executing the program module resource with the WAD to generate a signal (6; 4-14); (d4) storing the signal(s) in memory (6; 4-14); and (d5) generating a display with the WAD based on the signal generated in the substep (d4) (9; 1-8).

As per claim 15, Skopp teaches a method as claimed in claim 12, wherein the step (d) comprises the substeps of: (d1) receiving at the WAD via the network, a signal from the RDS generated based on execution of a server application by the RDS (9; 1-8); (d2) storing the received signal in the memory of the WAD (9; 1-8); (d3) generating with the WAD a display signal in the memory of the WAD (9; 1-8); (d4) generating a display with the WAD based on the display signal (9; 1-8); (d5) executing a client application with the WAD to generate a signal based on the signal from the RDS (9; 1-17); (d6) transmitting the signal(s) to the RDS via the network (9; 1-17).

As per claim 16, Skopp teaches a method as claimed in claim 12, further comprising the step of: (d7) receiving input data at the WAD from a user, the client application executed in step (d5) based on the input data (9; 1-17).

As per claim 21, Skopp teaches a method comprising the steps of: receiving a signal requesting access to a resource, the signal having a secure URL with secured resource access right data (9; 1-43); extracting an IP address from the secured resource access right data (9; 1-43); comparing the extracted IP address with the IP address included in a HTTP message of the request signal (9; 1-28, 10; 1-9); authenticating that the IP address of the secured resource access right data corresponds to the IP address of a device requesting access to the resource, based on the comparing of step (c) (9; 1-28, 10; 1-9).

As per claim 22, Skopp teaches a method as claimed in claim 21, further comprising the step of: terminating the request signal if the authenticating of step (d) indicates that the IP address of the secured resource access right data does not match the IP address extracted from the HTTP message (9; 1-28).

As per claim 39, Skopp teaches a method comprising the steps of: receiving via the Internet a request signal including a URL indicating a location of a resource, secured resource access right data indicating rights of a device to access the resource, and an IP address of the device (9; 1-28); determining whether access to the resource is to be provided to the device identified by the IP address, based on secured resource access right data included in the request signal (9; 1-28); and providing access to the resource to a device identified by the IP address if the determining of the step (c) indicates that access to the resource is to be provided (9; 1-28).

As per claim 40, Skopp teaches a method as claimed in claim 39, further comprising the step of: terminating the request signal if the determining of the step (b) indicates that access to the device is not authorized (9; 1-43).

As per claim 41, Skopp teaches a method as claimed in claim 39, wherein said step (c) comprises the substep of transmitting the resource to the device via the Internet (9; 1-28).

As per claim 42, Skopp teaches a method as claimed in claim 39 further comprising the step of: authenticating the request signal if an IP address of the URL in the request signal matches the URL of the device contained in the resource access right data of the request signal (9; 1-43).

As per claim 43, Skopp teaches a method as claimed in claim 39, further comprising the steps of: retrieving resource access right data from a database, the determining of step (b) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data (9; 1-43).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 4, 7, 17-20, 23-38, 44-52, and 55-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skopp in view of Graunke et al (U.S. 5,991,399).

As per claim 3, Skopp teaches a method as claimed in claim 1, but does not specifically teach the generation of hash data based on key data. Graunke teaches the creation of hashing functions based on key data (column 2, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to include key data into the parameters of creation of hash data, as taught by Graunke in the system of Skopp. The motivation for doing so lies in the fact that adding another method of creating a hash function further diversifies the existing hashing function, to lead to increased security. Both inventions are from the same field of endeavor, namely the limitation of access of certain data.

As per claim 4, Skopp-Graunke teaches a method as claimed in claim 3, wherein steps (a)-(c) are performed at a resource provider subsystem (RDS) (Skopp: figure 1B; column 4, lines 56-67; column 9, lines 1-43); the method further comprising the step of: transmitting the key data from the RPS to a resource distribution subsystem hosting the resource so that, if the secure URL is activated by the web access device to generate a request for the resource to the

RDS, the RDS can verify that the resource access right data has not been modified other than by the RPS (Graunke: column 1, line 50 – column 2, line 19).

As per claim 7, Skopp-Graunke teaches a method as claimed in claim 6, wherein the hash data is generated further using key data corresponding to the web access device and/or user thereof, the method further comprising the step of: (e) transmitting key data corresponding to the web access device and/or user thereof to a resource distribution subsystem hosting the resource so that, if the secure URL is activated by the web access device to generate a request for the resource to the RDS, the RDS can verify that the resource access right data has not been modified other than by the RPS (Skopp: column 9, lines 1-43; Graunke: column 1, line 50 – column 2, line 19).

As per claim 17, Skopp-Graunke teaches a method comprising the steps of: at a resource distribution subsystem (RDS), (a) receiving a signal requesting access to a resource from a web access device, the signal including at least a URL, resource access right data, and hash data (Skopp: 9; 1-43); verifying that the resource access right data as set by a RPS has not been changed, using the hash data (Graunke: column 1, line 50 – column 2, line 19); (c) if the verifying establishes that the resource access right data has not been changed, determining whether access to the resource is permitted to the WAD and/or user thereof based on the resource access right data (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43); and (d) if the resource access right data indicates that the WAD and/or user thereof is authorized to access the resource, permitting access to the resource to the WAD and/or user thereof (9; 1-17).

As per claim 18, Skopp-Graunke teaches a method as claimed in claim 17, wherein the resource access right data includes at least one of: an authorized IP address or IP address range

(9; 1-17); lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid (10; 53-59); and maximum reference data indicating a maximum number of times a WAD and/or user thereof can access a resource (10; 27-33).

As per claim 19, Skopp-Graunke teaches a method as claimed in claim 17, wherein the hash data is generated based on the URL, resource access right data, and key data, the method further comprising the step of: receiving key data from the RPS for use in verifying in step (b) that the resource access right data has not changed from establishment by the RPS (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43);

As per claim 20, Skopp-Graunke teaches a method as claimed in claim 17, wherein the key data includes a key and optionally at least one of a second URL identifying the RPS; start date/time data identifying a date and time at which a key is valid (Skopp: 10; 28-67); end date/time data identifying a date and time at which a key becomes invalid (Skopp: 10; 28-67); lifespan data indicating a period of time over which the key is valid (Skopp: 10; 28-67); key index data identifying the key from among a plurality of different keys (Graunke: column 1, line 50 – column 2, line 19); hash identifier data indicating to the RDS a hash algorithm to be performed to generate the hash data (Skopp: 9; 1-43); encryption data indicating an encryption model and/or algorithm used to encrypt and decrypt resource access right data; and format fields data indicating the number of fields in the signal requesting access to the resource.

As per claim 23, Skopp-Graunke teaches a method as claimed in claim 22, further comprising the steps of: if the authenticating of step (d) indicates that the IP address of the secure resource access right data matches the IP address of the device requesting access to the resource, obtaining a key corresponding to the IP address (Graunke: column 1, line 50 – column

2, line 19; Skopp: 9; 1-43); verifying whether the key is valid based on data corresponding to the key in a secure content key database (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43); generating hash data based on at least the IP address, URL, and key (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43); and verifying that the hash data generated in the step (g) matches the hash data included in the request signal received in the step (a) (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43);

As per claim 24, Skopp-Graunke teaches a method as claimed in claim 23, further comprising the steps of: terminating the request signal if the verifying of the step (h) indicates that the hash data generated in the step (g) does not match the hash data included in the request signal received in the step (a) (Skopp: 9; 1-43).

As per claim 25, Skopp-Graunke teaches a method as claimed in claim 23, further comprising the steps of: determining whether access to a resource is to be provided to a device identified by the IP address, based on the resource access right data based on the resource access right data included in the request signal (Skopp: 9; 1-17); retrieving the resource based on the URL included within the request signal (Skopp: 9; 1-17); and providing access to the resource to a device identified by the IP address if the determining of step (j) indicates that access to the resource is to be provided, based on the URL (Skopp: 9; 1-28).

As per claim 26, Skopp-Graunke teaches a method as claimed in claim 25, further comprising the steps of: retrieving resource access right data from a database (Skopp: 9; 1-43, 55-56), the determining of step (j) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data (Skopp: 9; 1-28).

As per claim 27, Skopp-Graunke teaches a method as claimed in claim 26 further comprising the steps of: terminating the request signal if the determining of the step (l) indicates that access to the resource is not to be provided based on the resource access right data included in the request signal (Skopp: 9; 1-43).

As per claim 28, Skopp-Graunke teaches a method as claimed in claim 26 wherein the resource access right data retrieved in step (k) includes maximum reference data and reference count data, the method further comprising the step of: incrementing the reference count data to indicate that access to the resource has been requested by the request signal (Skopp: 9; 50-65, 10; 27-50); comparing the incremented reference count data with the maximum reference count data (Skopp: 9; 50-65, 10; 1-8, 27-50); and providing access to the resource if the comparing step (o) indicates that the incremented reference count data does not exceed the maximum reference count data (Skopp: 9; 50-65, 10; 1-8, 27-50).

As per claim 29, Skopp-Graunke teaches a method as claimed in claim 26, wherein the resource access right data retrieved in the step (k) includes lifespan data for access to the resource indicated by the URL, the method further comprising the steps of: determining a time and date of receiving the request signal in step (a); comparing the lifespan data with the time and date of receiving the requesting signal; and determining that the IP address of the request signal is authorized to access the resource, if the comparing of the step (n) indicates that the time and date of receiving the request signal is within the lifespan data (Skopp: 9; 1-43, 10; 28-67).

As per claim 30, Skopp-Graunke teaches a method as claimed in claim 29, wherein the resource access right data retrieved in the step (k) includes URL/resource provider identification data, the method further comprising the step of: retrieving the resource from a RPS via the

Internet, based on the URL/resource provider identification data, the retrieved resource used to provide access to the resource in the step (k) (Skopp: 9; 1-43).

As per claim 31, Skopp-Graunke teaches a method as claimed in claim 30, wherein the resource access right data retrieved in the step (l) includes retrieval key data used to decrypt the resource retrieved in the step (p) (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

As per claim 32, Skopp-Graunke teaches a method comprising the steps of: receiving a signal requesting access to a resource, the request signal including a URL, secured resource access right data, and an IP address of a device requesting access to the resource, and hash data (Skopp: 9; 1-43); verifying whether key data is valid based on data corresponding to the key data in a secure content key database (Graunke: column 1, line 50 – column 2, line 19; column 7, lines 59-67); if the key data is verified as valid in step (b), generating hash data based on at least the IP address, URL, and the key data (Graunke: column 1, line 50 – column 2, line 19); and verifying that the hash data generated in step (c) matches the hash data included in the request signal received in the step (a) (Skopp: 9; 1-43).

As per claim 33, Skopp-Graunke teaches a method as claimed in claim 32, further comprising the steps of: terminating the request signal if the verifying of the step (d) indicates that the hash data generated in the step (c) does not match the hash data included in the request signal received in step (a) (Skopp: 9; 1-43).

As per claim 34, Skopp-Graunke teaches a method as claimed in claim 33, further comprising the steps of: determining whether access to a resource is to be provided to a device identified by the IP address, based on the resource access right data included in the request signal

(Skopp: 9; 1-43); and providing access to the resource to a device identified by the IP address if the determining of step (f) indicates that access to the resource is to be provided (Skopp: 9; 1-43).

As per claim 35, Skopp-Graunke teaches a method as claimed in claim 34, further comprising the steps of: retrieving resource access right data from a database (Skopp: 9; 55-56), the determining of step (f) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data (Skopp: 9; 1-43, 55-56).

As per claim 36, Skopp-Graunke teaches a method as claimed in claim 32, wherein the request signal received in step (a) includes key index data, the method further comprising the step of: retrieving the key data from the secure content key database using the key index data (Graunke: column 1, line 50 – column 2, line 19; column 7, lines 59-67).

As per claims 37 and 38, Skopp-Graunke teaches a method as claimed in claim 32, where a lifespan of a key is determined, and from this lifespan, the system determines whether access will be granted based on whether the time of the requests fall within the lifespan (Skopp: 10; 28-67). Skopp-Graunke does not specifically teach the retrieval and comparison of specific dates and times against specific dates and times for which a certain request will be valid. It would have been obvious to one of ordinary skill in the art at the time of the invention to include the specific noting of the time and date so that it can be compared in a database to a time and date for which the request will be valid, in view of Skopp's teaching of the lifespan data. To execute it specifically by noting date and time constitutes a design choice.

As per claim 44, Skopp-Graunke teaches a method as claimed in claim 29, further comprising the step of: verifying validity of key data (Graunke: column 1, line 50 – column 2); generating hash data based on at least the URL and the key data (Skopp: 9; 1-43); comparing the hash data generated in step (e) with hash data included in the received request signal (Skopp: 9; 1-43); determining whether the hash data generated in step (e) matches the hash data generated in the request signal, based on the comparing step of the step (f) (Skopp: 9; 1-43), the access to the resource provided in step (c) if the determining step (g) establishes that the hash data match (Skopp: 9; 1-43).

Claim 45 and 46 are rejected on the same basis as claims 37 and 38.

As per claim 47, Skopp-Graunke teaches a system using the Internet, the system comprising: at least one web access device executing a browser application, the WAD generating a signal requesting a web page document having a secure URL, receiving the web page document having the secure URL, displaying the web page document having the secure URL, and generating a signal requesting a resource indicated by the secure URL of the web page document (Skopp: 9; 1-43); a resource provider subsystem coupled to receive via the Internet the signal requesting the web page document from the WAD, the RPS generating the secure URL to include resource access right data defining restrictions of the WAD and/or user thereof to access the resource indicated by the URL, the RPS transmitting the web page document with the secure URL to the WAD (Skopp: 9; 1-43); and at least one resource distribution subsystem coupled to receive via the Internet the signal from the WAD requesting access to the resource, the RDS determining whether the resource access right data has been changed from establishment by the RPS, and if the RDS determines that the resource access right data has not

been changed, the RDS determining whether the WAD and/or user thereof is authorized to access the resource using the resource access right data, the RDS permitting access to the resource if the WAD and/or user thereof is authorized to access the resource (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

As per claim 48, Skopp-Graunke teaches a system as claimed in claim 47, wherein the resource access right data includes at least one of: an authorized IP address or an IP address range (Skopp: 9; 1-9); lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid (Skopp: 10; 53-66); and/or maximum reference data indicating a maximum number of times a WAD and/or user thereof can access a resource (Skopp: 10; 28-50).

As per claim 49, Skopp-Graunke teaches a system as claimed in claim 47, wherein the hash data is generated by the RPS based on the URL, resource access right data, and key data, and the RDS stores the key data used by the RPS, the RDS verifying that the resource access right data has not changed from establishment by the RPS using the key data (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

Claim 50 is rejected on the same basis as claim 20.

As per claim 51, Skopp-Graunke teaches a server storing a secure URL generator module executable by the server to generate a URL having secure resource access right data defining restrictions on a WAD and/or user thereof to access a resource indicated by the secure URL, the resource access right data secured by the server so that modification of the resource access right data can be detected (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

As per claim 52, Skopp-Graunke teaches a server as claimed in claim 51, wherein the server stores a secure content key database having key data, and the server executes the secure URL generator module to secure the resource access right data with the key data (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

As per claim 55, Skopp-Graunke teaches a server as claimed in claim 51 wherein the server comprises a resource access right database storing the resource access right data (Skopp: 9; 1-43).

As per claim 56, Skopp-Graunke teaches a server as claimed in claim 51, wherein the server comprises an access right enforcer module, the server executing the access right enforcer module to determine whether a resource is to be provided to another server in response to a request signal received from the other server via the Internet, the server executing a secure caching module to transmit the resource to the other server for distribution if the resource access right data indicates that the other server is authorized to access the resource, and the server preventing access to the other server if the resource access right data indicates the other server is not authorized to access the resource (Skopp: 9; 1-43).

As per claim 57, Skopp-Graunke teaches a server of a RDS storing an access right enforcer module executable by the server, the server executing the access right enforcer module in response to a signal from a WAD requesting access to a resource, the request signal having a URL with secure resource access right data, the server executing the access right enforcer module using resource access right data to determine whether the resource access right data has been modified after its establishment by a RPS, the server preventing access to the resource if the resource access right data has been modified after its establishment, the server further executing

a secure caching module if the resource access right data has not been modified to provide access to the resource if the WAD is determined by the server to have the right to access the resource based on the resource access right data, and the server blocking access to the resource if the WAD is determined not to have the right to access the resource (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

As per claim 58, Skopp-Graunke teaches a server as claimed in claim 57, wherein the request signal received by the server from the WAD includes an IP address, a URL indicating the location of the resource, and hash data, the server retrieving key data based on the IP address and/or URL, the server combining the key data with at least the IP address and/or URL, the server generating hash data based on the key data and IP address and/or URL, the server comparing the server-generated hash data with the hash data in the request signal, the server executing its secure caching module to provide access to the resource if the hash data matches, and the server blocking access to the resource if the hash data do not match (Graunke: column 1, line 50 – column 2, line 19; Skopp: 9; 1-43).

Claims 59 and 60 are rejected on the same basis as claims 37 and 38.

Claims 53 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skopp-Graunke in view of Gifford (U.S. 5,812,776).

As per claim 53, Skopp-Graunke teaches a server as claimed in claim 51, but does not specifically teach the appending of key data to an IP address to form a hash, and combining the hash with the URL to form a secure URL. Gifford teaches the combining of a hash into a URL to form a secure URL (column 4, lines 20-43). It would have been obvious to one of ordinary

skill in the art at the time of the invention to include the specific encryption of a URL by combining it with a hash, as taught by Gifford in the system of Skopp-Graunke. The motivation for doing so lies in the fact that having an encrypted URL would allow for further security of a website, such that hackers would face a stronger security scheme. All inventions are from the same field of endeavor, namely the securing of network resources.

As per claim 54, Skopp-Graunke-Gifford teaches a server as claimed in claim 51, wherein the server uses the key data to encrypt the resource access right data and combines the encrypted resource access right data with the URL to produce the secure URL (Gifford: 4; 20-43).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Levergood et al. (U.S. 5,708,780) teaches Internet server access control and monitoring systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tanim Hossain whose telephone number is 571/272-3881. The examiner can normally be reached on 8:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey can be reached at 571/272-3896. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tanim Hossain
Patent Examiner
Art Unit 2145

V. Martin Wallace
Supervisory Patent Examiner